PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-102020
(43)Date of publication of application : 15.04.1997

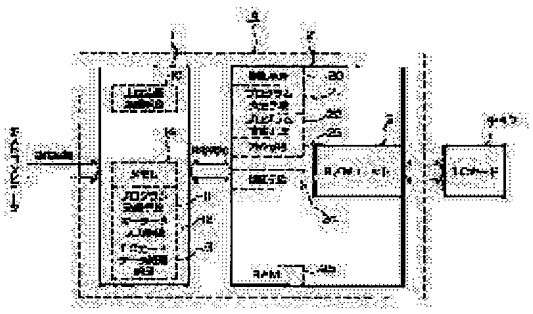
(51)Int.Cl. G06K 17/00
G06F 9/06

(21)Application number : 07-257999
(22)Date of filing : 04.10.1995

(71)Applicant : TOPPAN PRINTING CO LTD
(72)Inventor : HIRANO SEIJI
MATSUMURA SHUICHI
YURA AKIYUKI

(54) IC CARD TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an IC card terminal high in security and capable of easily altering a processing program.
SOLUTION: When the processing of an IC card authentication program NP starts, whether an IC card 4 is inserted into an R/W unit 3 or not is judged. Then, the activation of the I/C card 4 is detected based on ATR information. When the IC card 4 is an authenticating card 4', the propriety of the IC card 4, that of the IC card terminal A and that of a system are recognized. When they are judged to be impropriety in an authentication processing, an error flag is stored in RAM 25. When the IC card authentication processing is ended, the IC card 4 is discharged from the R/W unit 3 and a new IC card processing program IPQ is loaded.



LEGAL STATUS

[Date of request for examination] 09.09.2002
[Date of sending the examiner's decision of rejection] 05.07.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－102020

(43)公開日　平成９年(1997)４月15日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｅ	
Ｇ０６Ｆ　9/06	５５０		Ｇ０６Ｆ　9/06	５５０Ｋ	

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

(21)出願番号　特願平7－257999

(22)出願日　平成７年(1995)10月４日

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号

(72)発明者　平野　誠治
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

(72)発明者　松村　秀一
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

(72)発明者　由良　彰之
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

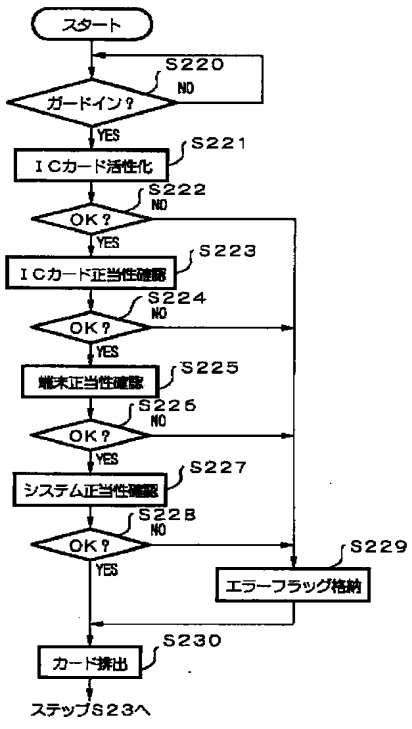
(74)代理人　弁理士　川▲崎▼　研二　（外１名）

(54)【発明の名称】　ＩＣカード端末

(57)【要約】

【課題】　セキュリティが高く、処理プログラムの変更が容易なＩＣカード端末を提供する。

【解決手段】　ＩＣカード認証プログラムＮＰの処理が開始すると、まず、Ｒ／ＷユニットにＩＣカード４が挿入されているか否かを判定し（Ｓ２２０）、その後、ＩＣカード４の活性化をＡＴＲ情報に基づいて検出する（Ｓ２２１）。ＩＣカード４が認証用カード４´であるならば、ＩＣカード４の正当性、ＩＣカード端末Ａの正当性、システムの正当性を確認する（Ｓ２２３～Ｓ２２８）。上記認証処理で不当と判定された場合には、エラーフラッグをＲＡＭ２５に格納する（Ｓ２２９）。こうして、ＩＣカード認証処理が終了すると、ＩＣカード４をＲ／Ｗユニット３から排出し（Ｓ２３０）、新たなＩＣカード処理プログラムＩＰＱをローディングする。



【特許請求の範囲】

【請求項１】　データの読出または書込のうち少なくとも一方をＩＣカードに対して行うＩＣカード端末において、

前記ＩＣカードに対応した処理プログラムを記憶する不揮発性の記憶手段と、

この処理プログラムを書き換える際、書換の正当性を認証する認証手段と、

この認証手段によって正当性が認証された場合に前記記憶手段に格納されている前記処理プログラムを書き換える書換手段と、

前記ＩＣカードに対してデータの読出または書込のうち少なくとも一方を行うインターフェース手段と、

前記処理プログラムに基づいて、前記インターフェース手段を制御する制御手段とを備えたことを特徴とするＩＣカード端末。

【請求項２】　前記認証手段は、認証用ＩＣカードの正当性を認証することを特徴とする請求項１に記載のＩＣカード端末。

【請求項３】　前記認証手段は、認証用ＩＣカードが前記ＩＣカード端末の正当性を認証した認証情報に基づいて、書換の正当性を認証することを特徴とする請求項１に記載のＩＣカード端末。

【請求項４】　前記認証手段は、暗号関数または復号関数を用いて、書換の正当性を認証することを特徴とする請求項１乃至３のいずれか１項に記載のＩＣカード端末。

【請求項５】　前記記憶手段、前記認証手段、前記書換手段、および前記制御手段を有する演算処理装置を備えたことを特徴とする請求項１乃至４のいずれか１項に記載のＩＣカード端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＣカード端末に関するものであり、特に、セキュリティが高く、また新たなＩＣカードにも対応できるシステムを構築するのに好適である。

【０００２】

【従来の技術】ＩＣカードは、内部に半導体メモリを有し、そこに大量の情報を記憶できしかも携帯に便利であることから、その利用分野は急速に拡大されつつある。これに伴い、用途に応じたＩＣカードが各種開発されつつある。これらのＩＣカードにあっては、そのクロック周波数や通信プロトコルが相違するのが通常である。したがって、新たなＩＣカードが開発されると、従来のＩＣカード端末では対応できず、その制御プログラムを変更する必要がある。

【０００３】

【発明が解決しようとする課題】ところで、この制御プログラムは、ＰＲＯＭやＣＰＵ内部のマスクＲＯＭに格

納されているか、あるいは、電話回線等の通信回線を介してＩＣカード端末内のメモリにローディングされる。

【０００４】しかし、ＰＲＯＭに制御プログラムを格納したのでは、ＰＲＯＭ自体が盗難された場合、制御プログラムを容易に読み出されてしまう。また、制御プログラムを変更するにはＰＲＯＭやＣＰＵを交換する必要があり、不便である。一方、制御プログラムを通信回線を介して配信する場合にあっては、第３者が通信回線を介してＩＣカード端末にアクセスする虞がある。このため、制御プログラムの偽造、改変等の可能性があり、セキュリティが低いという問題があった。

【０００５】本発明は上述した事情に鑑がみてなされたものであり、セキュリティが高く、かつ、制御プログラムの変更が容易なＩＣカード端末を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記課題を解決するため請求項１に記載のこの発明にあっては、データの読出または書込のうち少なくとも一方をＩＣカードに対して行うＩＣカード端末において、前記ＩＣカードに対応した処理プログラムを記憶する不揮発性の記憶手段と、この処理プログラムを書き換える際、書換の正当性を認証する認証手段と、この認証手段によって正当性が認証された場合に前記記憶手段に格納されている前記処理プログラムを書き換える書換手段と、前記ＩＣカードに対してデータの読出または書込のうち少なくとも一方を行うインターフェース手段と、前記処理プログラムに基づいて、前記インターフェース手段を制御する制御手段とを備えたことを特徴とする。

【０００７】また、請求項２に記載のこの発明にあっては、前記認証手段は、認証用ＩＣカードの正当性を認証することを特徴とする。また、請求項３に記載のこの発明にあっては、前記認証手段は、認証用ＩＣカードが前記ＩＣカード端末の正当性を認証した認証情報に基づいて、書換の正当性を認証することを特徴とする。

【０００８】また、請求項４に記載のこの発明にあっては、前記認証手段は、暗号関数または復号関数を用いて、書換の正当性を認証することを特徴とする。また、請求項５に記載のこの発明にあっては、前記記憶手段、前記認証手段、前記書換手段、および前記制御手段を有する演算処理装置を備えたことを特徴とする。

【０００９】

【発明の実施の形態】

１．実施形態の構成

以下、図面を参照してこの発明の実施形態の構成について説明する。図１はこの発明に係るＩＣカード端末が適用されるＩＣカードシステムの一実施形態のブロック図である。図１において、１はパーソナルコンピュータであり、通信回線を介して図示せぬホストコンピュータと接続されている。２はＩＦＤ回路であり、パーソナルコ

ンピュータ１と接続され、パーソナルコンピュータ１から送信される制御プログラムＳＰを受信し、この制御プログラムＳＰに基づいて、データの書込読出を行う。３はＲ／Ｗユニットであり、ＩＣカード４からデータを読み出し、また、データの書き込む。ＡはＩＣカード端末であり、上記したパーソナルコンピュータ１、ＩＦＤ回路２およびＲ／Ｗユニット３から構成される。なお、４´は認証用カードであり、プログラムを書き換える際に、その正当性を認証するために用いられる。

【００１０】次に、パーソナルコンピュータ１は、以下の部分により構成される。１０は上位装置通信手段であり、ホストコンピュータとのインタフェースであり、制御プログラムＳＰの受信や各種のデータ通信を行う。また、１１はプログラム送信手段であり、ＩＦＤ回路２に対して、制御プログラムＳＰをＲＳ２３２Ｃの形式で送信する。また、１２はキーボードで構成されるキーデータ入力手段であり、これにより、操作指示が入力される。また、１３はＩＣカードデータ処理手段であり、ＩＣカード４に格納すべきデータを暗号化し、またＩＣカード４から読み出したデータを復号化する。

【００１１】また、ＩＦＤ回路２は以下の部分により構成される。２０は制御手段であり、ＩＦＤ回路２の動作全体を制御する。２１はプログラム受信手段であり、パーソナルコンピュータ１から送信される制御プログラムＳＰを受信する。２２はプログラム書換手段であり、制御プログラムＳＰの一部または全部の書換を行う。２３はフラッシュメモリであり、書換可能で不揮発性である。フラッシュメモリ２３には、制御プログラムＳＰが格納される。２４は認証手段であり、制御プログラムＳＰの一部書換に際して、書換の正当性を認証する。２５はＲＡＭであり、制御手段２０の作業領域として機能する。

【００１２】ここで、フラッシュメモリ２３に格納される制御プログラムＳＰについて、図２を用いて説明する。図２はフラッシュメモリ２３のメモリマップである。同図示すように制御プログラムＳＰは、メインプログラムＭＰ、ＲＡＭ転送プログラムＲＰ、ＩＣカード処理プログラムＮＰ、書換プログラムＫＰおよびＩＣカード処理プログラムＩＰから構成される。

【００１３】まず、第１ブロックＢ１にはメインプログラムＭＰが格納される。このメインプログラムＭＰは、ＩＦＤ回路２をデータ読出・書込可能な状態にすると共に、所定の場合に書換プログラムＫＰを実行する。

【００１４】また、第２ブロックＢ２には、ＲＡＭ転送プログラムＲＰ、ＩＣカード認証プログラムＮＰおよび書換プログラムＫＰが格納される。ＲＡＭ転送プログラムＲＰは、所定のブロックに格納されているプログラムをＲＡＭ２５に転送するためのプログラムである。また、ＩＣカード認証プログラムＮＰは、ＩＣカードを用いて、ＩＣカードの正当性、端末の正当性およびシステムの正当性を確認するためのプログラムである。また、書換プログラムＫＰは、第３ブロックＢ３に格納されているプログラムを書き換えるためのプログラムである。

【００１５】また、第３ブロックＢ３には、ＩＣカード処理プログラムＩＰが格納される。ＩＣカード処理プログラムは、パーソナルコンピュータ１からのコマンドを受信し、そのコマンドの処理を行うためのプログラムである。なお、第１，第２ブロックＢ１，Ｂ２に格納されたプログラムは、動作処理の基本プログラムであるため、固定であるが、第３ブロックＢ３に格納されたプログラムは、対象とするＩＣカードのバージョンアップやシステム変更に対応できるように、書換可能である。

【００１６】次に、ＩＦＤ回路２の具体的な構成を図３を参照して説明する。図３はＩＦＤ回路の回路図である。同図において、２００はＣＰＵであり、上記した制御手段２０、プログラム書換手段２２、フラッシュメモリ２３、認証手段２４およびＲＡＭ２５として機能する。この例では、ＣＰＵ２００にＨ８／５３８Ｆ（日立製作所）を用いている。

【００１７】ＣＰＵ２００において、XTAL,EXTALはクロック入力端子であり、そこには4.9152ＭＨｚで発振する水晶振動子２０１が接続される。また、MD0,MD1,MD2は、動作モード端子であり、これらの接続状態によって、ＣＰＵ２００の動作モードが設定される。例えば、動作モード端子MD0,MD1,MD2に５Ｖが供給される場合には、通常モードとして動作する。通常モードにあっては、ＲＡＭ２５に格納されているプログラムを実行したり、フラッシュメモリ２３に格納されているプログラムの一部を書き換える。一方、動作モード端子MD0,MD1に５Ｖが供給されると共に動作モード端子MD2に１２Ｖが供給される場合には、ブートモードとして動作する。ブートモードでは、ＣＰＵ２００の内部にあるフラッシュメモリ２３に格納されているプログラムが全て消去され、プログラムの書込が再度行われる。

【００１８】また、Vppは、フラッシュメモリ２３の消去用電源供給端子であり、リセット出力端子を兼ねる。RESは、リセット端子であり、そこにローレベルが供給されるとＣＰＵ２００の動作は初期化される。なお、端子Vppに１２Ｖが供給されると、フラッシュメモリコントロールレジスタの第７ビットにフラッグが発生するよう構成されている。

【００１９】また、P60～P64は第６ポートの入出力端子、P72～P77は第７ポートの入出力端子である。このうち、端子P72,P73,P76,P77は、インターフェス手段２１０（MAX232）に接続されており、コネクタ２１１を介してパーソナルコンピュータ１とデータの交換を行う。具体的には、端子P72はシリアルデータを送信し、端子P73はシリアルデータを受信し、端子P76,P77はクロック信号を入出力する。なお、インターフェス手段２１０はシリアルデータとＲＳ２３２Ｃ形式データとを相互に変換

するものであり、上記したプログラム受信手段２１として機能する。

【００２０】また、端子P60～P64, P74, P75は、Ｒ／Ｗユニット３の各端子と接続される。すなわち、端子P61はリセット端子RESETと、端子P74, P75はデータの入出力を行うデータ入出力端子I/Oと、端子P62は電源端子Vccと、端子P63はカード入力信号を出力する端子CIと、端子P64はカード出力信号を入力する端子COと、端子60はＮＡＮＤ回路を介してクロック信号を入力する端子CLKと接続される。

【００２１】２．実施形態の動作

以下、図面を参照してこの発明の実施形態の動作について説明する。この実施形態の動作は、ブートモード動作、実行動作、書換動作に大別される。以下、場合を分かち説明する。

【００２２】２－１ブートモード動作

ブートモードでは、ＣＰＵ２００を制御する制御プログラムＳＰを初期書込する。以下、図４を参照してブートモード動作を説明する。

【００２３】まず、スイッチＳＷ３をＯＮ状態にしてリセット端子RESをローレベルにすると（ステップＳ１）、ＣＰＵ２００の動作が初期化される。そして、スイッチＳＷ１，ＳＷ２をＯＮ状態にすると（ステップＳ２）、動作モード端子MD2と端子Vppには１２Ｖが供給される。この後、スイッチＳＷ３をＯＦＦ状態にしてリセット端子RESをハイレベルにすると（ステップＳ３）、ＣＰＵ２００は、ブートモードに遷移し、フラッシュメモリ２３への書込データを受け付ける状態となる。

【００２４】次に、ステップＳ４に進み、パーソナルコンピュータ１から制御プログラムＳＰがプログラム送信手段１１（図１参照）を用いて送信されると、これがコネクタ２１１とインターフェス手段２１０とを介してＣＰＵ２００に供給され、その内部にあるフラッシュメモリ２３の各ブロックＢ１～Ｂ３に制御プログラムＳＰが書き込まれる。

【００２５】こうして、フラッシュメモリ２３には、第１ブロックＢ１にメインプログラムＭＰが、第２ブロックＢ２にＲＡＭ転送プログラムＲＰ、ＩＣカード認証プログラムＮＰおよび書換プログラムＫＰが、第３ブロックＢ３にＩＣカード処理プログラムＩＰがそれぞれ書き込まれる。

【００２６】２－２ 実行動作

実行動作では、設定される条件に応じて、ＩＣカード処理プログラムモードとユーザープログラムモードとを選択する。ＩＣカード処理プログラムモードではＩＣカード処理プログラムＮＰを実行し、ユーザープログラムモードでは書換プログラムＫＰを実行する。以下、図５を参照しつつ、実行動作を説明する。

【００２７】まず、スイッチＳＷ３をＯＮ状態にすると、リセット端子RESがローレベルとなり（ステップＳ１０）、ＣＰＵ２００の動作が初期化される。そして、スイッチＳＷ１をＯＦＦ状態にすると（ステップＳ１１）、動作モード端子MD2の電圧は５Ｖとなり、ＣＰＵ２００は通常モードに遷移する。この後、リセット端子RESをハイレベルにすると（ステップＳ１２）、ＣＰＵ２００は、フラッシュメモリ２３に格納されているメインプログラムＭＰをＲＡＭ２５に転送し、これを実行する。

【００２８】メインプログラムＭＰの処理が開始すると、まず、端子Vppの電圧が１２Ｖであるか否かが判定される（ステップＳ１３）。具体的には、フラッシュメモリコントロールレジスタの第７ビットにフラッグが存在するか否かによって、端子Vppに１２Ｖが供給されているか否かが判定される。

【００２９】スイッチＳＷ２がＯＮ状態であるならば、端子Vppの電圧が１２Ｖとなり、ステップＳ１３で「ＹＥＳ」と判定され、ステップＳ１４に進んで、ユーザープログラムモードに遷移する。ユーザープログラムモードとは、フラッシュメモリ２３に格納されているＩＣカード処理プログラムＩＰを書き換えるモードである。一方、スイッチＳＷ２がＯＦＦ状態であるならば、端子Vppの電圧は５Ｖとなり、ステップＳ１３で「ＮＯ」と判定され、ステップＳ１５に進んで、ＩＣカード処理モードに遷移する。以下、ユーザープログラムモードとＩＣカード処理モードとを場合を分かち詳述する。

【００３０】２－２－１ ユーザープログラムモード動作

図６はユーザープログラムモードのフローチャートである。同図において、まず、フラッシュメモリ２３から、その第２ブロックＢ２に格納されているＩＣカード認証プログラムＮＰと書換プログラムＫＰとをＲＡＭ２５に転送する（ステップＳ２０）。この転送が終了すると、ＣＰＵ２００はＲＡＭ２５に格納されたＩＣカード認証プログラムＮＰを実行し、その後、書換プログラムＫＰを実行する（Ｓ２１）。

【００３１】ステップＳ２２では、ＩＣカード認証プログラムＮＰを実行する。この動作を図７に示すＩＣカード認証プログラムＮＰのフローチャートを用いて説明する。ＩＣカード認証プログラムＮＰの処理が開始すると、まず、Ｒ／ＷユニットにＩＣカード４が挿入されているか否かを判定する（ステップＳ２２０）。具体的には、端子P63に供給されるカード入力信号の有無をＣＰＵ２００で検出する。ここで、ＩＣカード４が挿入されていなければ、「ＮＯ」を選択し、ＩＣカード４が挿入されるまでこの判定を繰り返す。

【００３２】そして、ＩＣカード４が挿入されると、「ＹＥＳ」を選択して、ＩＣカード４の活性化を検出する（ステップＳ２２１）。具体的には、図３に示す端子60をハイレベルにしてゲートを開きクロック信号を端子CLKに供給する。また、端子P62から電源を電源端子Vcc

に供給した後、端子P61をハイレベルにしてリセット信号をリセット端子RESETに供給する。この後、ＩＣカード４の種別を表すＡＴＲ情報がＲ／Ｗユニット３から出力されると、端子P74, P75に供給されるＡＴＲ情報を検出する。そして、ＡＴＲ情報が認証用カード４´を表しているか否かを判定し（ステップＳ２２２）、ＩＣカード４が認証用カード４´でない場合には、「ＮＯ」を選択し、ステップＳ２２９に進んで、エラーフラッグをＲＡＭ２５に格納し、ＩＣカード４を排出する（ステップＳ２３０）。これにより、認証用カード４´を用いなければ、ＩＣカード処理プログラムＩＰの書換を行うことができない。

【００３３】ＩＣカード４が認証用カード４´であるならば、「ＹＥＳ」を選択しステップＳ２２３に進み、ＩＣカード４の正当性を確認する。この動作シーケンスを図８を用いて説明する。まず、ＩＣカード端末Ａ内のＣＰＵ２００において、乱数Ａを発生し、これにキーＩＤを付加してＩＣカード４に送信する。キーＩＤは、ＩＣカード４に格納されている各種のＩＤの中から所定のＩＤを特定するための情報である。この場合のキーＩＤはカードＩＤを指示する。

【００３４】この後、ＩＣカード端末Ａ内のＣＰＵ２００は、カードＩＤを鍵Ｋ１として用い、乱数Ａを暗号化して乱数Ｂを生成する。ここで暗号関数をＥとすれば、乱数Ｂは、次式で表される。

Ｂ＝Ｅ（Ａ，Ｋ１）

【００３５】一方、ＩＣカード４にあっては、キーＩＤと乱数Ａを受信すると、内部のメモリをアクセスし、キーＩＤに基づいてカードＩＤを読み出す。そして、このカードＩＤを鍵Ｋ１´として用い、乱数Ａを暗号化して乱数Ｂ´を生成する。ここで用いられる暗号関数はＥであり、ＩＣカード端末Ａ内で用いられる暗号関数と同一である。乱数Ｂ´は、次式で表される。

Ｂ´＝Ｅ（Ａ，Ｋ１´）

【００３６】この後、乱数Ｂ´がＩＣカード４からＩＣカード端末Ａに送信されると、ＣＰＵ２００は乱数Ｂと乱数Ｂ´が一致するか否かを判定する。両者が一致するのは、同一の暗号関数、同一の鍵を用いて暗号化した場合であるから、この場合にはＩＣカード４は正当であると判定される。一方、乱数Ｂと乱数Ｂ´が不一致であれば、ＩＣカード４は不当であると判定される。

【００３７】このようにして、ＩＣカード４の正当性がＩＣカード端末Ａによって確認され、図７に示すステップＳ２２４に進む。そして、ＩＣカード４が不当な場合には、エラーフラッグをＲＡＭ２５に格納し（ステップＳ２２９）、ＩＣカード４をＲ／Ｗユニット３から排出する（ステップＳ２３０）。一方、ＩＣカード４が正当である場合には、ＩＣカード端末Ａの正当性を確認する（ステップＳ２２５）。この動作シーケンスを図９を用いて説明する。

【００３８】まず、ＩＣカード端末Ａ内のＣＰＵ２００が乱数要求を発生し、これをＩＣカード４に送信すると、ＩＣカード４の内部で乱数Ａを発生し、乱数ＡをＩＣカード端末Ａに返信する。これを受けたＩＣカード端末Ａは、端末ＩＤを鍵Ｋ２として用い、乱数Ａを暗号化して乱数Ｂを生成する。ここで暗号関数をＥとすれば、乱数Ｂは、次式で表される。

Ｂ＝Ｅ（Ａ，Ｋ２）

【００３９】この後、ＣＰＵ２００は、乱数Ｂにキーを付加してＩＣカード４に送信する。この場合のキーＩＤは端末ＩＤを特定する。乱数ＢとキーＩＤをＩＣカード４が受信すると、ＩＣカード４は内部のメモリをアクセスし、キーＩＤに基づいて端末ＩＤを読み出す。そして、この端末ＩＤを鍵Ｋ２´として用い、乱数Ｂを復号化して乱数Ａ´を生成する。ここで用いられる復号関数はＤであり、ＩＣカード端末Ａ内で用いられる暗号関数Ｅと相補的な関係にある。乱数Ａ´は、次式で表される。

Ａ´＝Ｄ（Ｂ，Ｋ２´）

【００４０】この後、ＩＣカード４は乱数Ａと乱数Ａ´が一致するか否かを判定する。両者が一致するのは、暗号関数と復号関数が相補的な関係にあり、同一の鍵を用いて暗号化・復号化した場合である。この場合にあっては、ＩＣカード４は、ＩＣカード端末Ａが正当であると判定し、正常を表すステータスＳＪをＩＣカード端末Ａに送信する。一方、乱数Ｂと乱数Ｂ´が不一致であれば、ＩＣカード４は、ＩＣカード端末Ａが不当であると判定し、異常を表すステータスＳＪをＩＣカード端末Ａに送信する。

【００４１】このようにして、ＩＣカード端末Ａの正当性がＩＣカード４によって確認され、図７に示すステップＳ２２６に進む。ここで、ＣＰＵ２００は、ステータスＳＪが正常か否かを判定し、異常あれば「ＮＯ」を選択して、エラーフラッグをＲＡＭ２５に格納し、ＩＣカード４をＲ／Ｗユニット３から排出する（ステップＳ２３０）。

【００４２】一方、ステータスＳＪが正常であれば「ＹＥＳ」を選択し、システムの正当性を確認する（ステップＳ２２８）。具体的には、作業者がキーボードを操作して暗証番号やシステムキーを入力すると、ＣＰＵ２００がその正当性を確認する。暗証番号やシステムキーが不当であれば「ＮＯ」を選択して、エラーフラッグをＲＡＭ２５に格納し、ＩＣカード４をＲ／Ｗユニット３から排出する（ステップＳ２３０）。一方、暗証番号やシステムキーが正当であれば、認証動作を終了し、ＩＣカード４をＲ／Ｗユニット３から排出する（ステップＳ２３０）。

【００４３】こうして、ＩＣカード認証処理が終了すると、図６に示すステップＳ２３に進んで、プログラムの書換を行うか否かを判定する。具体的には、ＲＡＭ２５

にエラーフラッグが格納されているか否かによって判定し、エラーフラッグが格納されていれば「ＮＯ」を選択し、ステップＳ２２に戻る。一方、エラーフラッグが格納されていなければ「ＹＥＳ」を選択し、ステップＳ２５に進む。

【００４４】ステップＳ２５では、フラッシュメモリ２３の第３ブロックＢ３に格納されているＩＣカード処理プログラムＩＰを消去する。この後、パーソナルコンピュータ１が、新たなＩＣカード処理プログラムＩＰＱを送信すると、これを受信してＲＡＭ２５に一旦格納する（ステップＳ２５）。この例にあっては、通信フォーマットにモトローラＳフォーマットを用いる。このモトローラＳフォーマットでは、送信の際に付加したアドレスが、通信データを格納すべきフラッシュメモリ２３上の領域を指示する。

【００４５】この後、ＲＡＭ２５から当該ブロックにＩＣカード処理プログラムＩＰＱを転送し、その書込を行う（ステップＳ２６）。書込終了後、ＩＣカード処理プログラムＩＰＱのベリファイを行う（ステップＳ２７）。ただし、ＲＡＭ２５の容量には制限があるので、上記ステップＳ２５～Ｓ２７の処理は、所定バイト単位で行われる。このため、ステップＳ２８では、ＩＣカード処理プログラムＩＰＱについて全処理が終了したか否かを判定する。未処理である場合には、「ＮＯ」と判定され、ステップＳ２５からステップＳ２８までの処理を繰り返す。そして、全処理が終了すると、「ＹＥＳ」と判定され、ステップＳ２９に進んで、スイッチＳＷ２をＯＦＦ状態にする。これにより、端子Vppが５Ｖとなり、ステップＳ１４のユーザープログラムモード（図５参照）が終了し、ＩＣカード処理プログラムが変更される。

【００４６】２－２－２　ＩＣカード処理モード動作

次に、ＩＣカード処理モード動作を図１０を参照しつつ説明する。図１０はＩＣカード処理モードのフローチャートである。まず、パーソナルコンピュータ１から送信されるコマンドをＩＦＤ回路２が受信すると（ステップＳ３０）、そのコマンドに基づいてＩＣカードコマンド処理を行うか否かを判定する（ステップＳ３１）。具体的には、コマンドの先頭コードを参照する。この例にあっては、先頭コードが２Ｅｈの場合が、ＩＣカードコマンド処理を指示する。したがって、先頭コードが２Ｅｈであれば「ＹＥＳ」を選択し、ＩＣカードコマンド処理を実行する（ステップＳ３２）。

【００４７】ＩＣカードコマンド処理ではＩＣカード４に対してデータ読出・書込を行う。例えば、受信したコマンドがデータ読出を指示する場合にあっては、アプリケーションで使用するファイルをＩＣカード４にアクセスして選択し、鍵の照合を行い、この後、データをＩＣカード４からデータを読み出す。なお、データ読出に際して、キーボードからパスワードを入力し、鍵の照合を行っても良い。

【００４８】また、受信したコマンドがデータ書込を指示する場合にあっては、アプリケーションで使用するファイルをＩＣカード４にアクセスして選択し、鍵の照合を行い、この後、データをＩＣカード４へデータを書き込む。なお、データ書込に際して、キーボードからパスワードを入力し、鍵の照合を行っても良い。

【００４９】一方、コマンドの先頭コードが２Ｅｈでなく、ＩＣカードコマンド処理を指示しない場合にあっては、ステップＳ３１で「ＮＯ」と判定され、ステップＳ３３に進んで、Ｒ／Ｗコマンド処理が実行される。ここでは、パーソナルコンピュータ１から受信したコマンドに基づいて、カード排出やカード挿入待等の処理を行う。

【００５０】こうして、ＩＣカードコマンド処理（ステップＳ３２）またはＲ／Ｗ制御コマンド処理（ステップＳ３３）が終了すると、その処理結果をパーソナルコンピュータ１に対して出力する（ステップＳ３４）。これを受けてパーソナルコンピュータ１は、新たな指示をＩＦＤ回路２に対して出力するか、処理を終了するかを判断する。新たな指示を出す場合にはステップＳ３０に戻り、ステップＳ３０～ステップＳ３４の処理を繰り返す。

【００５１】以上説明したようにこの実施形態によれば、ＣＰＵ２００の内部にあるフラッシュメモリ２３にＩＣカード処理プログラムＩＰを格納するので、第３者はＩＣカード処理プログラムＩＰを容易に読み出すことができない。また、ＩＣカード処理プログラムＩＰは、書換の正当性を認証した後でなければ、書き換えないので、セキュリティを向上させることができる。また、新たなＩＣカード処理プログラムＩＰＱをホストコンピュータから送信し、オンボード上で書換を行うので、ＰＲＯＭやＣＰＵの交換が不要となり、ＩＣカード処理プログラムＩＰの変更が容易となる。

【００５２】３．変形例

本発明は上述した実施形態に限定されるものでなく、例えば以下のように種々の変形が可能である。

【００５３】①上記実施形態において、ブートモード時の書込は、パーソナルコンピュータ１から制御プログラムＳＰを受信して書き込んでいたが、ＲＯＭライタを用いて書き込んでも良い。

【００５４】②上記実施形態において、ＩＣカード処理プログラムＩＰの書換には、ＩＣカードの正当性確認（ステップＳ２２３）、端末の正当性確認（ステップＳ２２５）およびシステム正当性確認（ステップＳ２２７）を全て行ったが、このうちのいずれか１つ、または、これらを適宜組み合せて行っても良い。また、ＩＣカードの正当性確認と端末の正当性確認とを同時に行う相互認証であっても良い。

【００５５】③上記実施形態において、認証処理に用い

る暗号関数・復号関数は（図８，９参照）、例えば、ＤＥＳ，ＦＥＡＬの他、配送鍵方式の一方式であるＲＳＡであっても良い。

【００５６】④上記実施形態において、ＩＣカード４は、マルチアプリケーションに対応するものであっても良い。すなわち、このＩＣカードは、複数の通信プロトコルや複数のコマンドコード，パラメータに対応する。この種のＩＣカードにあっては、ファイル選択と鍵照合が同一コマンドであり、これを実行した後、データを読み出すコマンドを実行すれば、所定のデータを読み出せるＩＣカードも存在する。このため、上述したＩＣカードコマンド処理において（図１０ ステップＳ３２参照）、コマンドをそのまま送信するようにしても良い。

【００５７】⑤上記実施形態において、新たなＩＣカード処理プログラムＩＰＱを認証用カード４´に格納し、書換の正当性が認証されたならば、そこからＩＣカード処理プログラムＩＰＱをＩＣカード端末Ａにローディングしても良い。

【００５８】

【発明の効果】以上説明したように、請求項１乃至５に記載した発明によれば、認証手段で書換の正当性が認証された場合に処理プログラムを書き換えるので、セキュリテイを向上させることができる。特に、請求項５に記載の発明にあっては、演算処理装置の内部に認証手段と記憶手段を備えるから、ＩＣカード端末が盗難されても、処理プログラムを読み出すことができないため、セキュリテイを大幅に向上させることができる。また、処理プログラムは書換可能であるため、新たなＩＣカードが開発された場合にも迅速に対応することができる。

【図面の簡単な説明】

【図１】　この発明の一実施形態のブロック図である。

【図２】　同実施形態におけるフラッシュメモリのメモリマップである。

【図３】　同実施形態における各ＩＣカードの通信フォーマットを示す説明図である。

【図４】　同実施形態に用いられるＩＦＤ回路の回路図である。

【図５】　同実施形態におけるブートモード動作を説明するためのフローチャートである。

【図６】　同実施形態における実行動作を説明するためのフローチャートである。

【図７】　同実施形態におけるＩＣカード認証プログラムのフローチャートである。

【図８】　この発明の他の実施形態を説明するためのフローチャートである。

【図９】　一のＩＣカードに対応したＡＴＲ情報のタイミングチャートである。

【図１０】　他のＩＣカードに対応したＡＴＲ情報のタイミングチャートである。

【符号の説明】

４　ＩＣカード

４´　認証用カード

３　Ｒ／Ｗユニット（インターフェース手段）

２２　プログラム書換手段（書換手段）

２３　フラッシュメモリ（記憶手段）

２４　認証手段

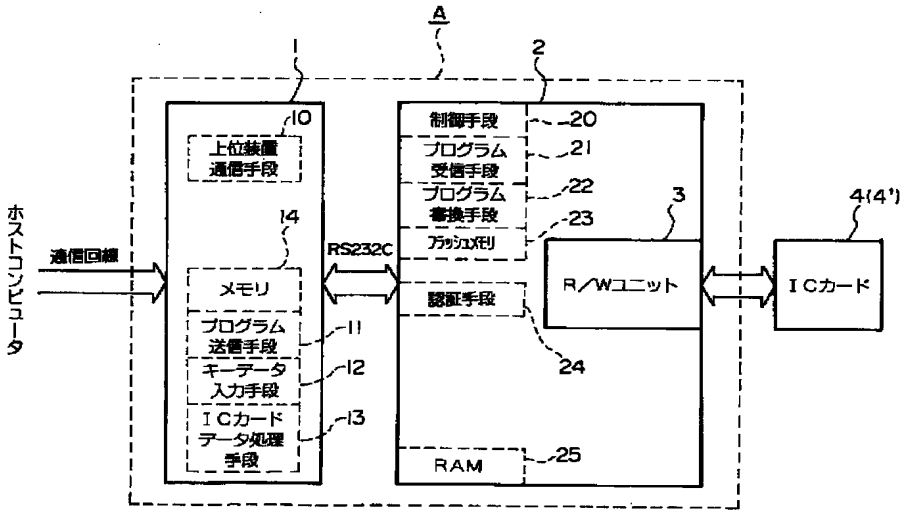
２００　ＣＰＵ（制御手段，書換手段，認証手段，記憶手段，演算処理装置）

Ａ　ＩＣカード端末

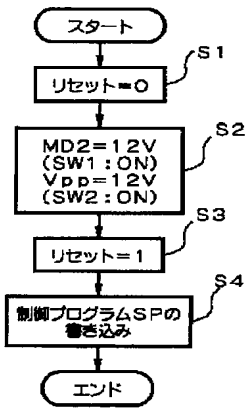
ＩＰ　ＩＣカード処理プログラム（処理プログラム）

ＳＪ　ステータス（認証情報）

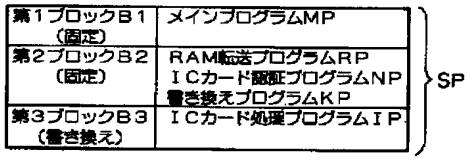
【図１】



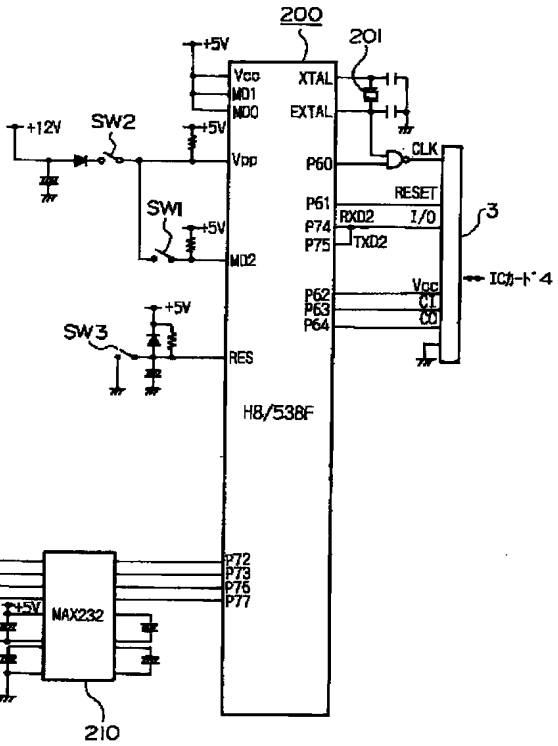
【図４】



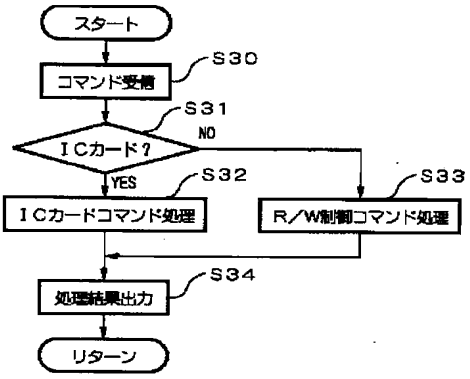
【図２】



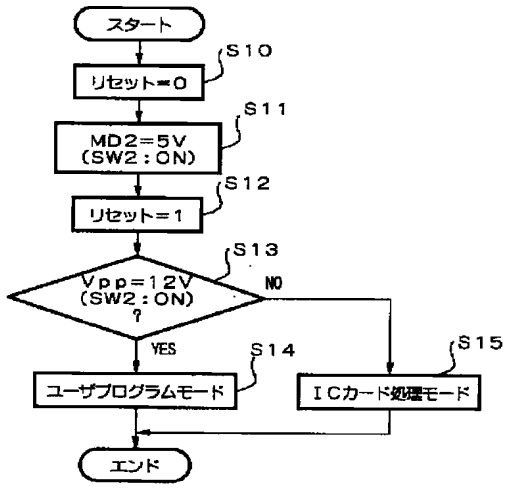
【図３】



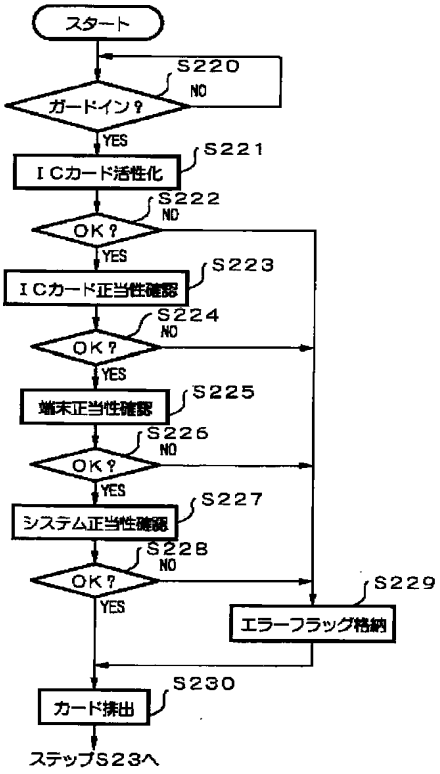
【図１０】



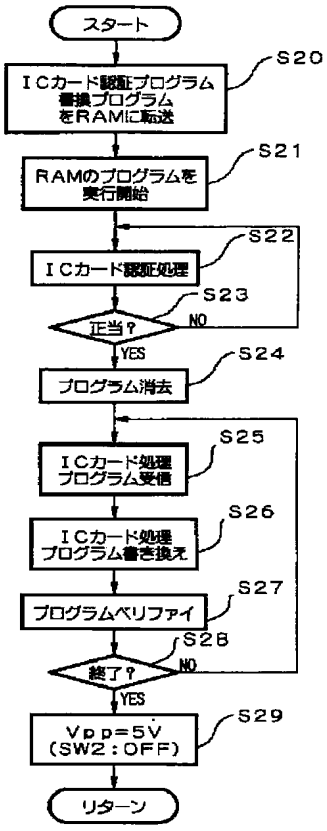
【図５】



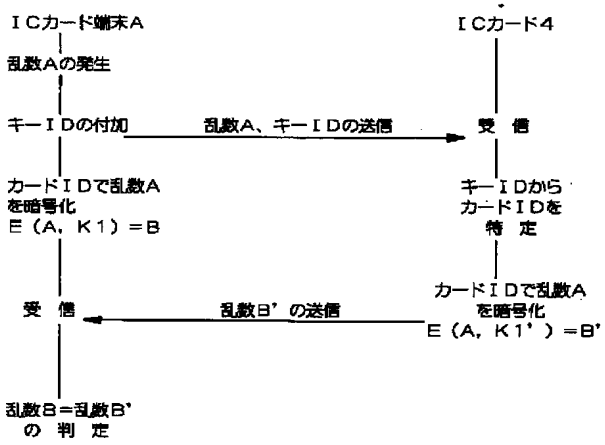
【図７】



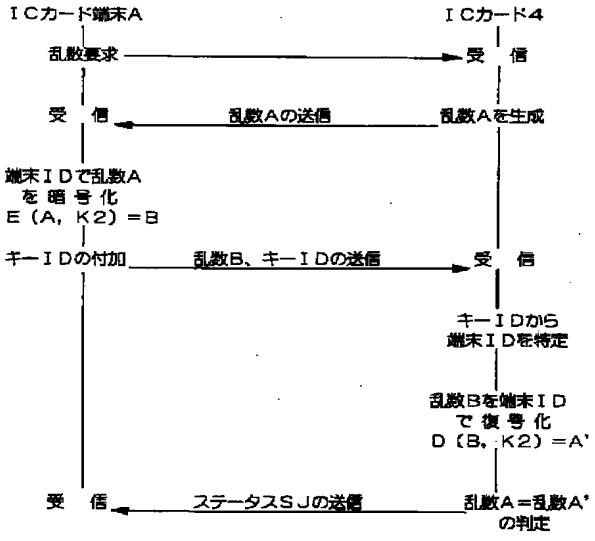
【図６】


スタート
ＩＣカード認証プログラム
書換プログラム
をRAMに転送
S20
RAMのプログラムを
実行開始
S21
ＩＣカード認証処理
S22
正当？
S23
NO
YES
プログラム消去
S24
ＩＣカード処理
プログラム受信
S25
ＩＣカード処理
プログラム書き換え
S26
プログラムベリファイ
S27
終了？
S28
NO
YES
Vpp=5V
(SW2：OFF)
S29
リターン

【図８】


ＩＣカード端末A
ＩＣカード4
乱数Aの発生
キーＩＤの付加
乱数A、キーＩＤの送信
受　信
カードＩＤで乱数A
を暗号化
E（A，K1）＝B
キーＩＤから
カードＩＤを
特　定
カードＩＤで乱数A
を暗号化
E（A，K1'）＝B'
受　信
乱数B'の送信
乱数B＝乱数B'
の　判　定

【図９】


ＩＣカード端末A
ＩＣカード4
乱数要求
受　信
受　信
乱数Aの送信
乱数Aを生成
端末ＩＤで乱数A
を暗号化
E（A，K2）＝B
キーＩＤの付加
乱数B、キーＩＤの送信
受　信
キーＩＤから
端末ＩＤを特定
乱数Bを端末ＩＤ
で復号化
D（B，K2）＝A'
受　信
ステータスSJの送信
乱数A＝乱数A'
の判定